UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/671,949	09/27/2000	Steven R. Tugenberg	GE04592	8330

22863 7590 06/22/2005

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
1L01/3RD
SCHAUMBURG, IL 60196

EXAMINER
NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/671,949	**Applicant(s)** TUGENBERG ET AL.	
	Examiner Abdulhakim Nobahar	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 11/02/04

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-21 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-21 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' response received on November 11, 2004.

2. The amendments of claims 1, 12 and 19 are acknowledged.

3. Amendment to specification is acknowledged and claim rejections under 35 USC § 112 are withdrawn.

4. Applicants' arguments have been fully considered but they are not persuasive.

5. Applicants argue that: "...encryption and decryption is performed directly using the laser-scribed encryption key as the encryption/decryption key. This is in contrast to Cassagnol et al., '727, which uses a session key, in addition to a master key and a device key, for purposes of encrypting and decrypting the data, at least some of which can not be said to equivalent to an/or obvious modifications of a laser-scribed encryption key associated with the secure processing system for a communication device, as provided by the claims of the present application."

Although Cassagnol teaches the use of one key for encryption and another key for decryption of the sensitive data, but it is apparent to a person of ordinary skill in the art that a symmetric technique of cryptography can readily be used instead of using a cryptography scheme with two keys (see, for example, Cassagnol at col. 7, line 63-col. 8, line 20; col. 3, lines 55-63 and Jenssen at col.5, lines 49-54).

6. In light of the above submission the previous rejection of claims is maintained with consideration of the amendments of claims 1, 12 and 19.

Previous rejection:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and are rejected under 35 U.S.C. 103(a) as being unpatentable over Janssen et al. (5,954,817; hereinafter Janssen) in view of Cassagnol et al. (6,385,727 B1; hereinafter Cassagnol).

Claims 1, and 12

Janssen discloses:

A secure processing system for a communication device (see col. 2, lines 10-41; Fig. 1) comprising:

a host processor (col. 3, lines 3-25); and a secure memory (col. 3, lines 3-25, ROM 210) coupled to the host processor (col. 3, lines 3-25, microprocessor 208) by a data bus (col. 3, lines 3-25, bus 220), wherein the secure memory comprises:

a laser-scribed encryption key (col. 3, line 58-col. 4, line 6);

encryption logic circuitry (col. 1, lines 45-53; col. 3, lines 14-25) for implementing a symmetric encryption algorithm using the laser-scribed encryption key (col. 2, lines 18-31; col. 3, lines 58-65; col. 5, lines 10-25);

a plurality of blocking gates coupling the encryption logic circuitry with the laser-scribed encryption key (col. 3, line 64-col. 4, line 6, where disabling access to the secret key indicates that the memory system also includes logic gates coupled to the logic circuit as described in the mentioned U.S. patent application Ser. No. 08/730,188 now U.S. patent No. 5,809,544); and

a memory (i.e., a non-secure memory coupled to host processor for storing encrypted data) (col. 3, lines 20-25),

Janssen, however, does not expressly disclose:

sensitive data is encrypted by the encryption logic circuitry directly using the laser-scribed encryption key and stored as encrypted data in a data storage medium, and

the encrypted data is decrypted by the encryption logic circuitry directly using the laser-scribed encryption key and transferred to the memory for use by the host processor.

Cassagnol teaches a secure processing environment (see abstract) that includes non-volatile memory, a logic circuit for controlling access to the data contained in the non-volatile memory directly connected to a key isolation circuit, and a number of logic gates (col. 3, lines 37-55; col. 12, lines 16-25). Cassagnol further discloses an external memory for storing encrypted data (col. 9, lines 16-20). Cassagnol teaches that the encrypted data is imported from the external storage medium to the internal memory and decrypted to be used by the processor and re-encrypted for storage in the external memory (col. 3, lines 56-63; col. 4, lines 42-61; col. 9, lines 21-40; Fig. 2).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the encryption of sensitive data for exporting to and importing from an external memory as taught in Cassagnol in the method of Janssen using the laser-scribed key, because it would prevent unauthorized use of sensitive data by hackers (col. 8, lines 28-40).

Claim 2

Cassagnol teaches:

wherein the memory is a zeroizable memory having a zeroizing input that causes the contents of the memory to be erased when a zeroize signal is received on the zeroizing input (see col.14, lines 10-33, where the erasable memory corresponds to the recited zeroizable memory and the means to trigger erasure of the memory corresponds to the recited zeroizing input), and wherein said zeroize signal is sent to the zeroizable memory by a system monitor upon the occurrence of one of a plurality of predetermined conditions (col. 12, lines 13-25; col. 13, lines 15-50).

Claim 3

Janssen discloses:

The processing system as claimed in claim 1 wherein the host processor and secure memory are fabricated on an integrated circuit chip, and the encrypted data is stored in a non-volatile memory (col.3, lines 20-42).

Claim 4

Janssen discloses:

The processing system as claimed in claim 3 wherein the non-volatile memory includes a portion internal to the integrated circuit chip and a portion external to the integrated circuit chip, and wherein the encrypted data is stored on the portion internal to the integrated circuit chip when the portion internal is available (See Fig. 2, where the non-volatile memory ROM 210 and ROM 210 are internal to the integrated circuit and non-volatile memory EEPROM is external).

Claim 5

Janssen discloses:

The processing system as claimed in claim 1 wherein the blocking gates are comprised of logic gates and have a blocking control signal input preventing access to the laser-scribed encryption key by the encryption logic circuitry (col. 3, line 58-col. 4, lines 6).

Claim 5

Cassagnol teaches:

The processing system as claimed in claim 1 wherein the blocking gates are comprised of logic gates and have a blocking control signal input preventing access to the laser-scribed encryption key by the encryption logic circuitry (col. 12, lines 15-25; col. 17, lines 15-30).

Claim 6

Janssen discloses:

The processing system as claimed in claim 1 wherein the laser-scribed encryption key is stored in a one-time programmable memory element (col. 3, lines 58-63).

Claim 7

Janssen discloses:

The processing system as claimed in claim 1 wherein the laser-scribed encryption key is stored in non-volatile memory selected from one of the group consisting of ROM, EEPROM, MRAM (Magnetoresistive RAM), battery backed RAM or DRAM and fast logic (col. 3, lines 58-63, where the memory 211 in Fig. 2 is a non-volatile ROM).

Claim 8

Janssen discloses:

The processing system as claimed in claim 1 wherein the laser-scribed encryption key is generated by laser-scribing a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser scribed encryption key, and

wherein the laser-scribed encryption key has a value that is randomly generated and is unique for each secure memory of a plurality of secure memories of different processing systems (col. 1, lines 35-53; col. 3, lines 58-66).

Claim 8

Cassagnol discloses:

The processing system as claimed in claim 1 wherein the laser-scribed encryption key is generated by laser-scribing a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser scribed encryption key, and

wherein the laser-scribed encryption key has a value that is randomly generated and is unique for each secure memory of a plurality of secure memories of different processing systems (col. 3, lines 50-55; col. 5, line 45-col. 6, line 2; col. 12, lines 58-64; col. 30, lines 38-42).

Claim 9

Janssen discloses:

The processing system as claimed in claim 1 wherein the laser-scribed encryption key is generated by burning one-time programmable fuses on a semiconductor die to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key, and

wherein the laser-scribed encryption key has a value that is randomly generated and is unique for each secure memory of a plurality of secure memories of different processing systems (col. 3, lines 55-66).

Claim 10

Janssen discloses:

The processing system as claimed in claim 1 wherein the symmetric encryption algorithm is a block cipher encryption algorithm (col. 2, lines 10-30; col. 5, lines 14-24).

Claim 10

Cassagnol discloses:

The processing system as claimed in claim 1 wherein the symmetric encryption algorithm is a block cipher encryption algorithm (col. 8, lines 5-20; col. 8, lines 35-40).

Claims 11 and 13

Cassagnol discloses:

The processing system as claimed in claim 1 wherein the host processor is coupled to an external memory (i.e., non-secure memory) having a secret key stored therein in encrypted form, the secret key being encrypted with the laser scribed encryption key, and said secret key being used for secure communication between the communication device and other communication devices (col. 3, line 64-col. 4, line 6; col. 10, lines 37-65).

Claim 14

Cassagnol discloses:

The communication device as claimed in claim 12 wherein the communication device is a data communication device, and wherein the secret key is a private key unique to a user of the communication device and is part of a public-private key pair, the private key being used for decrypting data sent to said user, and wherein prior to using said secret key, said secret key being decrypted by encryption logic of the secure memory using the laser-scribed encryption key and stored in unencrypted form in a zeroizable memory (col. 12, lines 13-25; col. 13, lines 15-50; col. 14, lines 10-33; col. 19, lines 60-67; col. 20, lines 49-61).

Claim 15

Janssen discloses:

The communication device as claimed in claim wherein the data communication device is adapted for transmitting data to another communication device, and wherein the secret key is further used to generate a digital signature associated with said data, said digital signature being transmitted along with said data (col. 2, lines 18-65).

Claim 16

Janssen discloses:

The communication device as claimed in claim 12 wherein the communication device is a wireless communication device for communicating secured voice, and wherein the secret key is used for generating a common session key for communicating with another communication device, and wherein prior to using said secret key, said secret key being decrypted by encryption logic of the secure memory using the laser-scribed encryption key and stored in unencrypted form in zeroizable memory (col. 1, lines 45-57; col. 2, lines 32-65).

Claim 17

Cassagnol discloses:

The communication device as claimed in claim 12 wherein the secret key is one of a plurality of secret encryption keys stored in encrypted form in the non-secure memory, the plurality of secret keys being encrypted with the laser-scribed encryption key, and

wherein one of the secret keys of the plurality is selected for secure communication between the communication device and other communication device, and wherein a zeroizable memory is cleared after communication with the other communication device, and

wherein prior to using said selected secret key, said selected secret key is decrypted by the encryption logic using the laser-scribed encryption key and stored in unencrypted form in the zeroizable memory (col. 3, line 64-col. 4, line 6; col. 12, lines 13-25; col. 13, lines 15-50; col. 14, lines 10-33; col. 19, lines 60-67; col. 20, lines 49-61).

Claim 18

Cassagnol discloses:

The communication device as claimed in claim 12 wherein the secure memory further comprises:

a plurality of blocking gates coupled to the laser-scribed encryption key (col. 12, lines 15-25);

encryption logic circuitry for implementing a symmetric encryption algorithm using the laser-scribed encryption key and coupled to the blocking gates (col. 13, lines 51-65); and

a zeroizable memory coupled to the encryption logic circuitry (see col. 14, lines 10-33, where the erasable memory corresponds to the recited zeroizable memory),

wherein sensitive data is encrypted by the encryption logic circuitry using the laser-scribed encryption key and stored as encrypted data in the non secure memory, and wherein the encrypted data is decrypted by the encryption logic circuitry with the laser-scribed encryption key and transferred to the zeroizable memory for use by the host processor (col. 4, lines 42-61; col. 9, lines 21-40; Fig. 2).

Claim 19

Janssen discloses:

A method of using secure information utilizing a secure communication device (see col. 2, lines 10-41; Fig. 1), the secure communication device comprising a host processor (col. 3, lines 3-25), a secure memory coupled to the host processor by a data bus (col. 3, lines 3-25), and a non-secure memory coupled to host processor for storing encrypted data (col. 3, lines 3-25), wherein the secure memory includes a laser-scribed encryption key stored therein (col. 2, lines 18-31; col. 3, lines 58-65; col. 5, lines 10-25).

Janssen, however, does not expressly disclose:

encrypting sensitive data within the secure memory directly using the laser-scribed encryption key;

storing the encrypted sensitive data in the non-secure memory;

decrypting the encrypted sensitive data within the secure memory directly using the laser-scribed encryption key; and

storing the decrypted sensitive data within the secure memory for use by the host processor.

Cassagnol teaches a secure processing environment (see abstract) that includes non-volatile memory, a logic circuit directly connected to a key isolation circuit for controlling access to the data contained in the non-volatile memory, and a number of logic gates (col. 3, lines 37-63; col. 12, lines 16-25). Cassagnol further discloses an external memory for storing encrypted data (col. 9, lines 16-20). Cassagnol teaches that the encrypted data is imported from the external storage medium to the internal memory and decrypted to be used by the processor and re-encrypted for storage in the external memory (col. 4, lines 42-61; col. 9, lines 21-40; Fig. 2).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the encryption of sensitive data for exporting to and importing from an external memory as taught in Cassagnol in the method of Janssen using the laser-scribed key, because it would prevent unauthorized use of sensitive data by hackers (col. 8, lines 28-40.

Claim 20

Cassagnol discloses:

The method as claimed in claim 19 wherein the secure memory includes blocking gates coupled between encryption logic circuitry and the laser-scribed encryption key (col. 12, lines 15-25), and a zeroizable memory coupled to the encryption logic circuitry (see col. 14, lines 10-33, where the erasable memory corresponds to the recited zeroizable memory), and wherein the storing step comprises storing the decrypted sensitive data within the zeroizable memory (col. 4, lines 42-61; col. 9, lines 21-40; Fig. 2), and wherein the method further comprises the steps of:

disabling the blocking gates during the encrypting and decrypting steps (col. 12, lines 15-25; col. 17, lines 15-30); and

zeroizing the zeroizable memory after the host processor is through using the decrypted sensitive data stored in the zeroizable memory (col. 12, lines 13-25; col. 13, lines 15-50).

Claim 21

Cassagnol discloses:

The method as claimed in claim 20 further comprising the step of enabling the blocking gates preventing the encryption logic circuitry from accessing the laser scribed encryption key, the step of enabling being performed upon completion of the decrypting step (col. 12, lines 15-25).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN a.n.
June 17, 2005

Gilberto Barron

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100